Descrição de Projeto
ICS-CERT Nacional

São Paulo, Setembro de 2015

TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Apresentação

Leonardo Cardoso

leonardo.cardoso@tisafe.com

- Gerente Regional da TI Safe Segurança da Informação para as regiões N/NE/CO
- Analista de Sistemas, com especialização em segurança da informação, também atua como perito em TICs junto ao TRT – Região 5
- Com larga experiência adquirida ao longo de 20 anos de atuação na área
- Escreve para mídias como Imasters, Websinder UOL, A Tarde e Bahia Notícias
- Conselheiro do CDI – Comitê para Democratização da Internet

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Mapa de Atuação

- **Escritórios**
  - ⇨ Rio de Janeiro
  - ⇨ São Paulo
  - ⇨ **Salvador**

- **Representantes Comerciais**
  - ⇨ Porto Alegre
  - ⇨ Brasília
  - ⇨ Goiânia
  - ⇨ Manaus
  - ⇨ Bogotá (Colômbia)

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Agenda

- Introdução às infraestruturas críticas e ciberterrorismo
- Principais desafios para 2015, 2016, 2017,…
- Riscos em redes industriais e SCADA
- ICS – CERT NACIONAL
- Conclusão
- Dúvidas?

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Infraestruturas Críticas e Ciberterrorismo

www.tisafe.com

TI Safe Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

O que são infraestruturas críticas de um país?

- São sistemas de infraestrutura para os quais a continuidade é tão importante que a perda, interrupção significativa ou degradação dos serviços trará graves consequências sociais ou à segurança nacional.
- Exemplos:
  - Geração e distribuição de eletricidade;
  - Telecomunicações;
  - Fornecimento de água;
  - Produção de alimentos e distribuição;
  - Aquecimento (gas natural, óleo combustível);
  - Saúde Pública;
  - Sistemas de Transportes;
  - Serviços financeiros;
  - Serviços de Segurança (polícia, exército)

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Portaria 45/2009 - GSI

GABINETE DE SEGURANÇA INSTITUCIONAL

PORTARIA Nº 45, DE 8 DE SETEMBRO DE 2009

Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, no uso de suas atribuições e tendo em vista o disposto no art. 4º do Decreto nº 4.801, de 06 de agosto de 2003, a autorização do Excelentíssimo Senhor Presidente da República e a deliberação do Comitê Executivo da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), em reunião realizada em 08 de outubro de 2008, CONSIDERANDO:

as informações tratadas no âmbito da Administração Pública Federal como ativos valiosos da nação, na nova concepção mundial de segurança e eficiência do Estado;

a crescente utilização de recursos de tecnologia da informação e comunicações na prestação de serviços públicos como instrumento democrático necessário ao acesso do cidadão às informações de governo, conferindo maior transparência à gestão do Estado, ao mesmo tempo em que aumenta a vulnerabilidade e tentativas de ataques às redes governamentais e bancos de dados, afetando a Administração Pública Federal;

o aumento das ameaças e tentativas de ataques cibernéticos, os quais incluem potenciais ataques às redes governamentais e banco de dados, afetando a Administração Pública Federal;

a necessidade de assegurar, dentro do espaço cibernético, ações de segurança da informação como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal;

a possibilidade real de uso dos meios computacionais para ações ofensivas contra as redes de computadores de instituições estratégicas do Governo Brasileiro, resolve:

Art. 1º Fica instituído o Grupo Técnico de Segurança Cibernética com o objetivo de propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal.

Art. 2º Considera-se Segurança Cibernética a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas.

§ 1º São Ativos de Informação os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

§ 2º São Infraestruturas Críticas as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009

O risco da falta de capacidade técnica

BRASIL

Editor-coordenador
Geraldo Bastos (interino)

brasil@grupoatarde.com.br

RS Polícia prende foragido condenado por tráfico internacional de pessoas www.atarde.com.br

ELETRICIDADE Diálogos gravados revelam o "sufoco" vivido pelos técnicos durante uma pane ocorrida em fevereiro de 2011

Operadores inaptos para lidar com apagão

ALANA RIZZO E IURI DANTAS
Agência Estado, Brasília

Diálogos inéditos entre operadores do sistema elétrico revelam despreparo nas subestações e centros de controle para enfrentar interrupções no fornecimento. As transcrições constam dos relatórios da Agência Nacional de Energia Elétrica e do Operador Nacional do Sistema, obtidos pelo jornal O Estado de S. Paulo por meio da Lei de Acesso à Informação.

Elas mostram o "sufoco" dos técnicos durante apagão em fevereiro de 2011, que deixou oito estados do Nordeste sem luz por horas. À época, o governo Dilma Rousseff atribuiu o apagão a um defeito em uma placa eletrônica. Nos minutos seguintes ao blecaute, os técnicos batiam cabeça. Faltou energia para abrir um portão e conseguir religar alguns equipamentos. Foi preciso quebrar a fechadura, atrasando a solução.

A subestação desconhecia como proceder e foi preciso ir atrás do manual de instruções em cima da hora. "É porque a gente tem que pegar o guia aqui porque não tem como acessar, aí estamos pegando o guia do normativo aqui e vamos fazer com ele", diz uma gravação. Quando o abastecimento de todo o NE dependia só da abertura de uma chave, como previa o guia de operações, os técnicos discutiam se, em vez de abrir como previa o rito normal, não era melhor fechar essa mesma chave. "Tá dependendo tudo, tem risco até de inundação na usina IV, tem que fechar", respondeu o Centro de Operações.

Assunto é divulgado graças à Lei de Acesso à Informação. Relatórios são conhecidos quando as expectativas para 2013 não são das melhores

Duas horas após iniciado o apagão, o Centro Regional de Operações da Companhia Hidro Elétrica do São Francisco questionou o técnico da subestação de Sobradinho se lá havia um equipamento chamado mesa de sincronismo. "Funciona não. Vou chamar um rapaz para ver se liga ela, muitos anos sem ligar, viu, chamo você depois".

Lista de falhas

O relatório da Aneel lista as irregularidades. Além do portão travado, havia aparelhos fora de operação, disjuntores fechados, discrepâncias no sistema de supervisão e controle e dificuldade de acesso aos procedimentos operacionais para a recomposição da instalação. A placa que apresentou defeito, dando origem ao apagão deveria ter sido substituída quatro anos antes, segundo relatórios. Responsável pela fiscalização das concessionárias, a Aneel não verificou se o equipamento fora efetivamente trocado. Tampouco sabia que duas usinas não tinham a máquina para religamento automático, para casos como aquele. Ao final, coube à agência reguladora pôr no papel o relato de uma sucessão de problemas facilmente evitáveis. Os erros renderam à Chesf uma multa de R$ 32 milhões.

Renasic

Gerar e endereçar o Plano de Ação Nacional para o cenário SCADA

Painel SCADA 2014

Rede Nacional de Segurança da Informação e Criptografia

Centro de Defesa Cibernética do Exército Brasileiro – CDCiber

Relatório 2 – Segurança em Sistemas de Controle e Automação Industrial das Infraestruturas Críticas: Plano de ações para o Brasil

http://www.renasic.org.br/content/files/2014_07_31_3/Painel_SCADA_2014_Relat%C3%B3rio_2_Plano_de_acoes.pdf

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Ataques aéreos – 1ª Guerra Mundial

- Aviões foram usados em combate pela primeira vez na primeira guerra mundial
- Trunfo: podiam bombardear a infraestrutura crítica de nações sem serem atingidos
- Na época, causaram grande terror à população e aos governos

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Ciber Guerra

- Cyber War ou Guerra Cibernética é (conceitualmente) <u>apenas uma nova modalidade da guerra convencional</u>.
- Principais diferenças:
  - Silenciosa
  - Anônima
  - Sem território definido
  - Sem reação
  - Quem? Como? De onde?

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yahweson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yahweson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"So shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and initiated by hackers."

Yahweson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 8-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"So dangerous as this technology is right now, it's going to get much worse," Yahweson said.

"Soon it will be sold to terrorists right and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yahweson

HACKERS PODEM TRANSFORMAR SEU PC EM UMA BOMBA

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Guerra Convencional X Guerra Cibernética

Quanto custa um bombardeiro Stealth **$1.5 a $2 bilhões**

Quanto custa um caça Stealth? **$80 a $120 milhões**

Quanto custa um míssil de cruzeiro **$1 a $2 milhões**

Quanto custa uma cyber arma? **$300 a $50,000**

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Encontre as armas de destruição em massa:

Fábricas de armas nucleares

Fábricas de cyber-armas

Onde estão as fábricas de cyber armas?

TI Safe Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Os novos atacantes

- Silenciosos
  - Sem alarmes, sem vestígios
- Precisos
  - Personalização, códigos específicos
  - Tomam vantagem sobre fraquezas tecnológicas e humanas
- Patrocinados
  - Por governos
  - Por empresas concorrentes
  - Por empresas de hacking
  - Por grupos terroristas

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Ciberterroristas

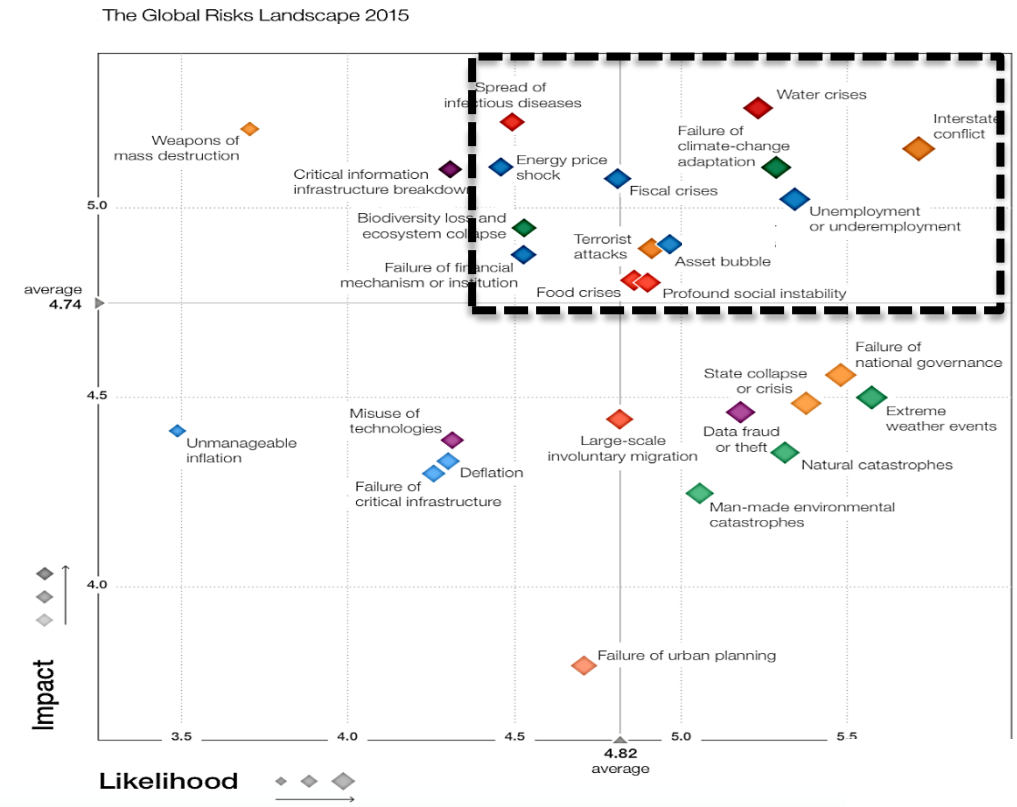
- Grupos organizados custeados por governos de países ou organizações terroristas para promover o terrorismo ao redor do mundo.
- A infraestrutura crítica dos países é o alvo preferido destes grupos.
- Enquanto hackers se preocupam em roubar ativos da empresa, Ciberterroristas se dedicam a promover atos de destruição.
- Cyber-Jihad e Cyber Al-Qaeda são exemplos.

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Principais desafios de 2015, 2016, 2017,…

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Relatório Global de Riscos 2015



ALTO IMPACTO
ALTA PROBABILIDADE

www.tisafe.com

TI Safe Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Desafios corporativos - ESG

Business and Security Initiative Priorities

© 2015 by The Enterprise Strategy Group, Inc.

Principais riscos

em redes industriais

TI Safe
Segurança da Informação

www.tisafe.com

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Algo em comum e diferenças de um ataque em ambientes de TI e TA

TI (informação)	TA (automação)
Infecção, domínio e controle.	Infecção, domínio e controle.
Lentidão de sistemas.	Lentidão de sistemas.
Paralisação de escritórios.	Paralisação de plantas.
Perda financeira, danos à imagem e passivo jurídico.	Perda financeira, danos à imagem e passivo jurídico.
	?
	?
	?

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Algo em comum e diferenças de um ataque em ambientes de TI e TA

TI (informação)	TA (automação)
Infecção, domínio e controle.	Infecção, domínio e controle.
Lentidão de sistemas.	Lentidão de sistemas.
Paralisação de escritórios.	Paralisação de plantas.
Perda financeira, danos à imagem e passivo jurídico.	Perda financeira, danos à imagem e passivo jurídico.
	Explosão e perda de ativos.
	Desastre ambiental.
	Morte.

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

As vezes só dá tempo de correr

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

ICS

INDUSTRIAL CONTROL SYSTEM

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

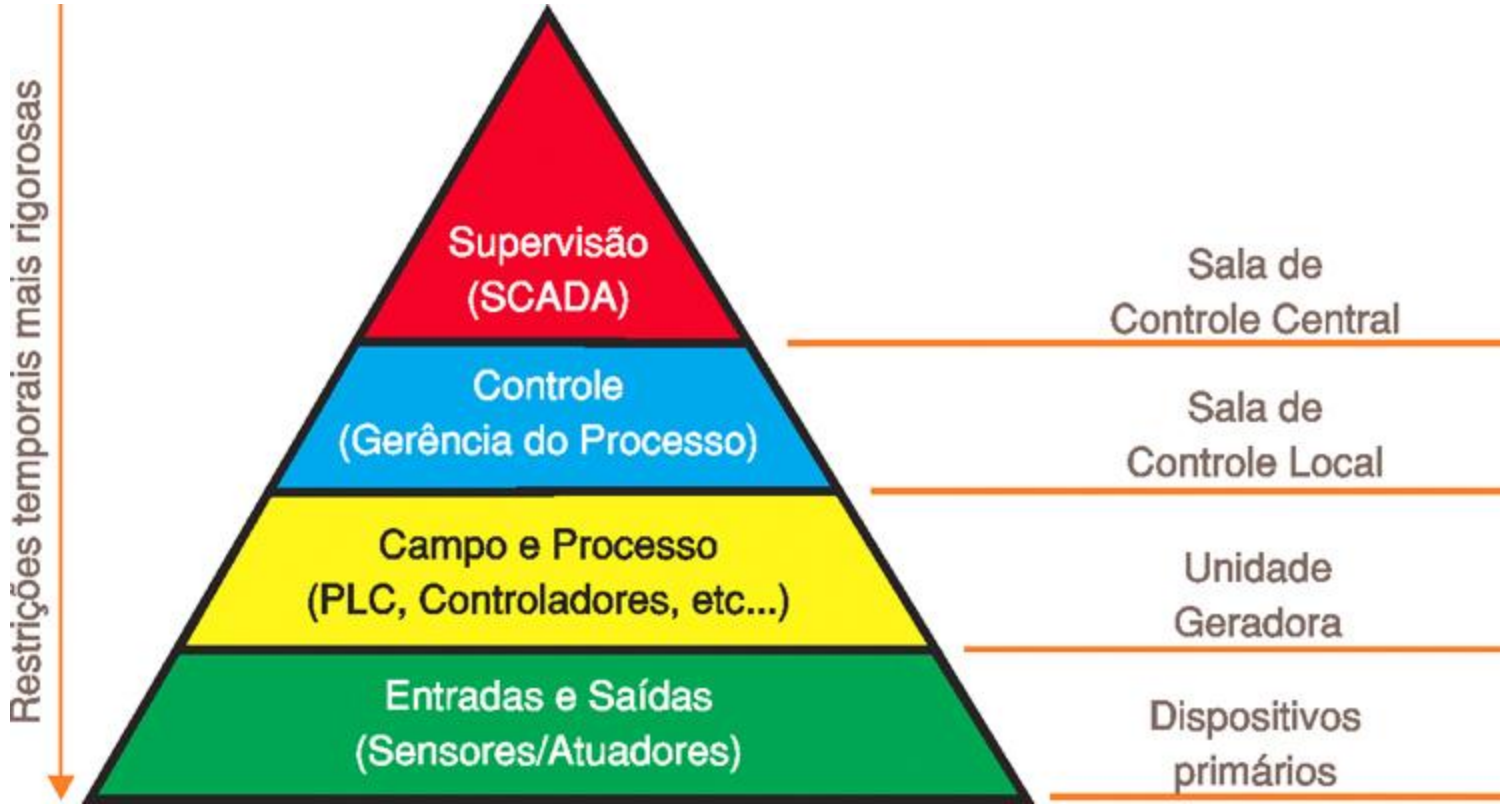
SCADA

Supervisory **C**ontrol **A**nd

Data **A**cquisition

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Pirâmide de Automação - Sistemas



TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

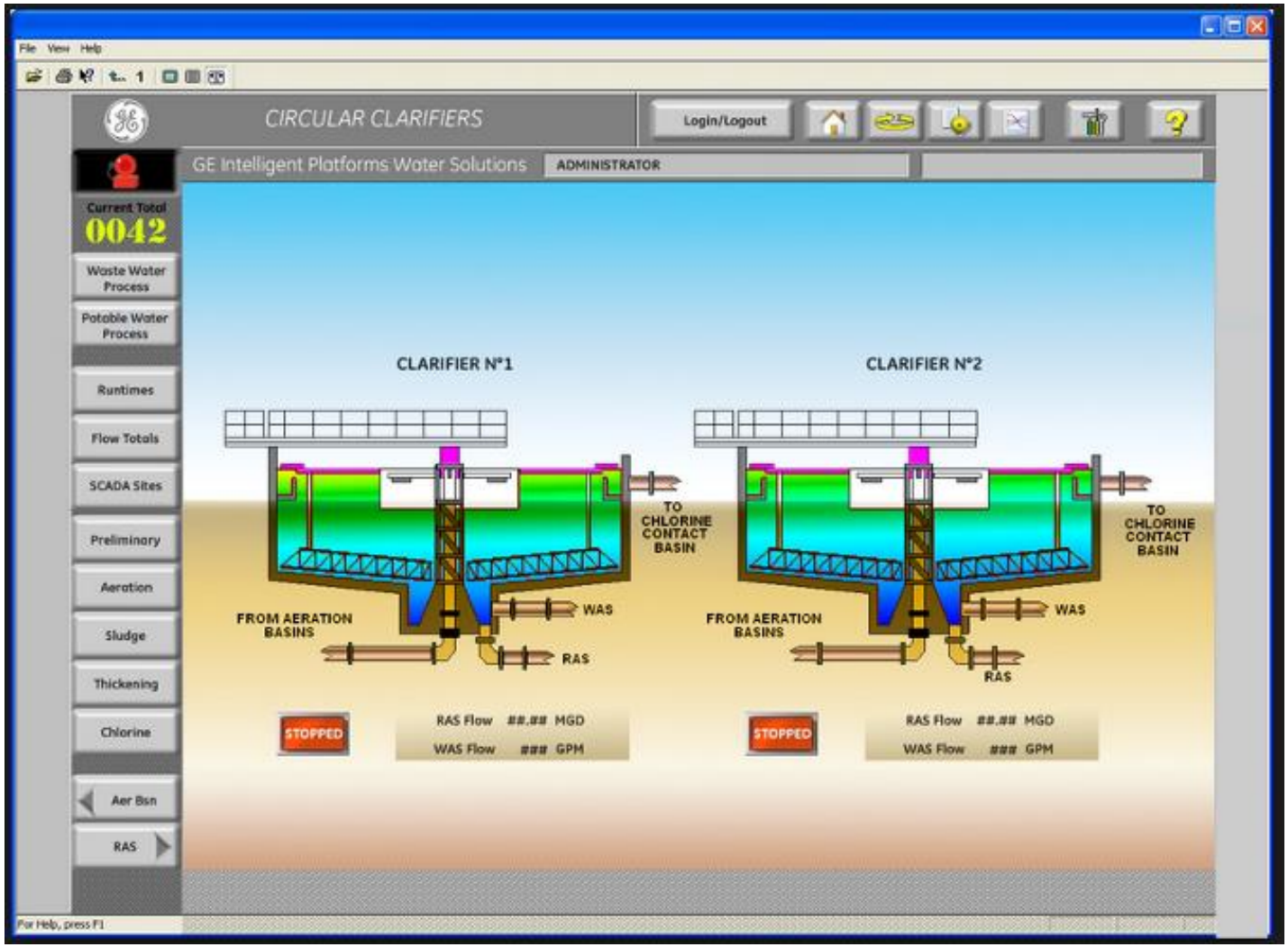
Como é a tela de controle de um Sistema SCADA

TI Safe
Segurança da Informação

www.tisafe.com

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Telas de operação de Sistemas SCADA

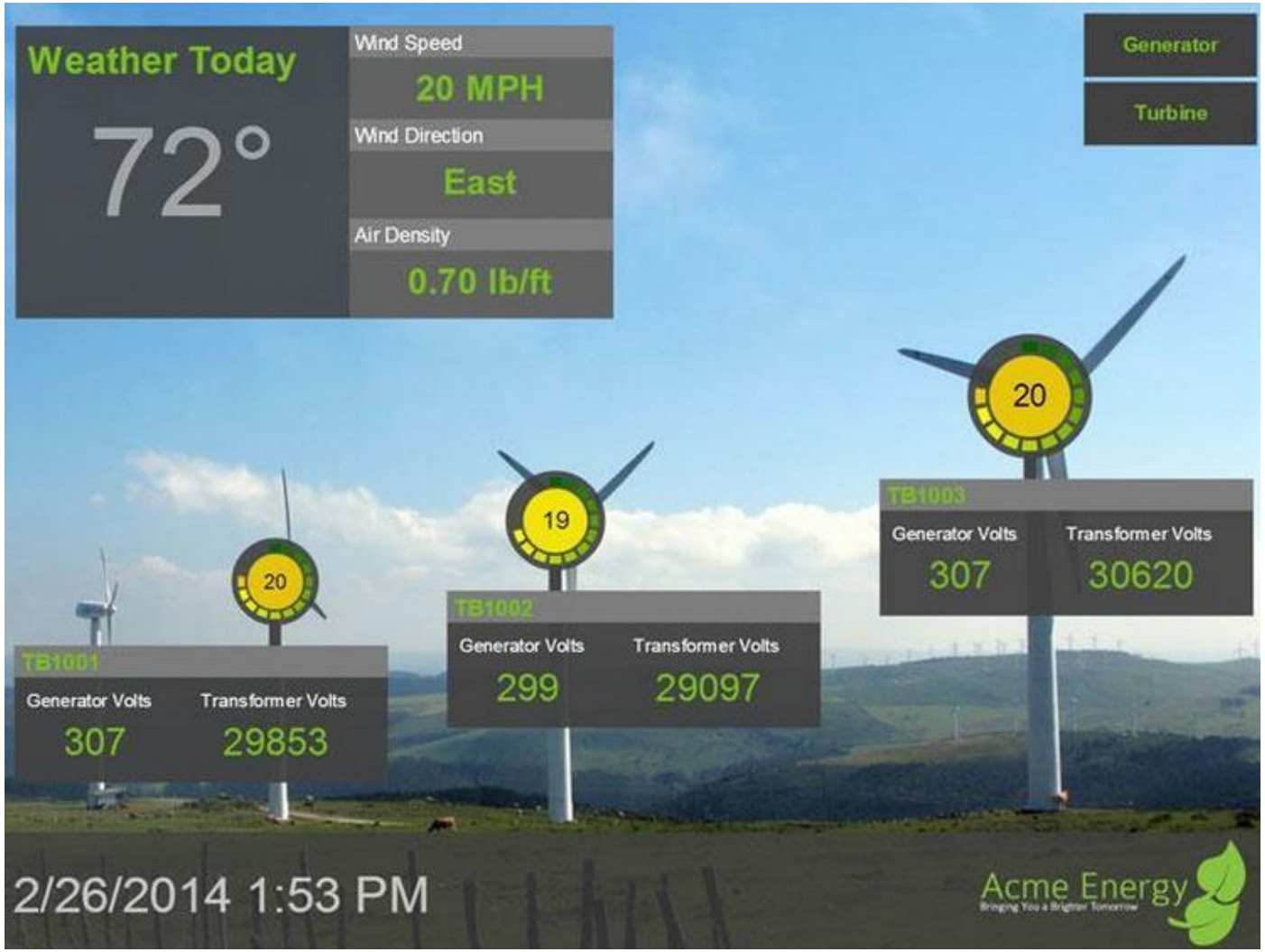


www.tisafe.com

TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Como é a tela de controle de um Sistema SCADA



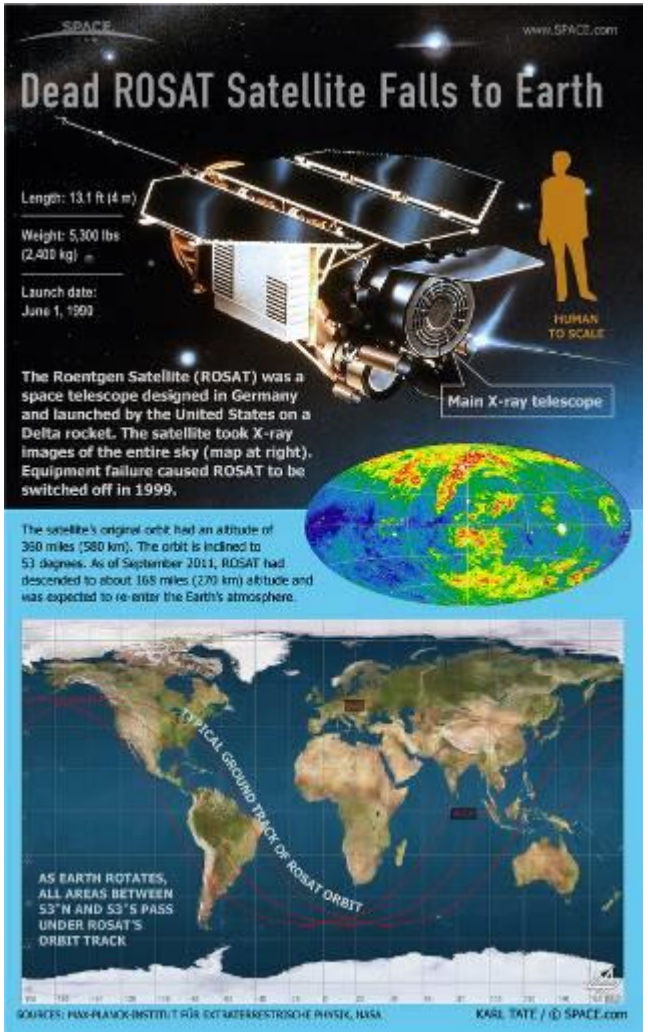
TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

INCIDENTES

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Ataque a centro de comando derruba satélite

- Em 2008 investigadores da NASA reportaram que uma falha no ROSAT estava ligada à uma cyber invasão no Goddard Space Flight Center, centro de comando do satélite.
- Segundo o relatório da NASA: “Atividades hostis comprometeram sistemas de computadores que direta ou indiretamente lidam com o controle do ROSAT”
- Após sucessivas falhas nos meses seguintes, em 23/10/11 o satélite alemão ROSAT explodiu ao reentrar na atmosfera terrestre. Seus destroços caíram em áreas inabitadas do planeta não causando vítimas.



TiSafe
Segurança da Informação

Bomba lógica destrói oleoduto na Sibéria

- Em 1982, durante a guerra fria, os planos de um sofisticado sistema SCADA para controle de oleoduto foram roubados pela KGB de uma empresa canadense.
- A CIA alega que esta empresa detectou o ataque e inseriu uma bomba lógica no código roubado para sabotar e explodir o oleoduto.
- A explosão foi equivalente a um poder de 3 Quilotons de TNT. A explosão foi tão poderosa que satélites americanos enviaram alertas nucleares aos centros de controle nos EUA.

A necessidade imediata do

ICS-CERT NACIONAL

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

ICS-CERT Nacional

Integrar empresas,

autoridades e governo

certificando todos os atores

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Foco em Segurança SCADA

- **Missão**
  - ⇨ Fornecer produtos e serviços de qualidade para a Segurança cibernética de Infraestruturas Críticas
- **Visão**
  - ⇨ Ser referência de excelência em serviços de Segurança cibernética de redes de infraestruturas criticas
- Equipe técnica altamente qualificada
- Parceria com grandes fabricantes mundiais

www.tisafe.com

Ti Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

TI Safe

ICS.SecurityFramework

DETECÇÃO, DEFESA E CONTROLE INTEGRADO DE AMEAÇAS PARA SISTEMAS INDUSTRIAIS

ISA

ANSI/ISA.99

NIST

NIST 800-82

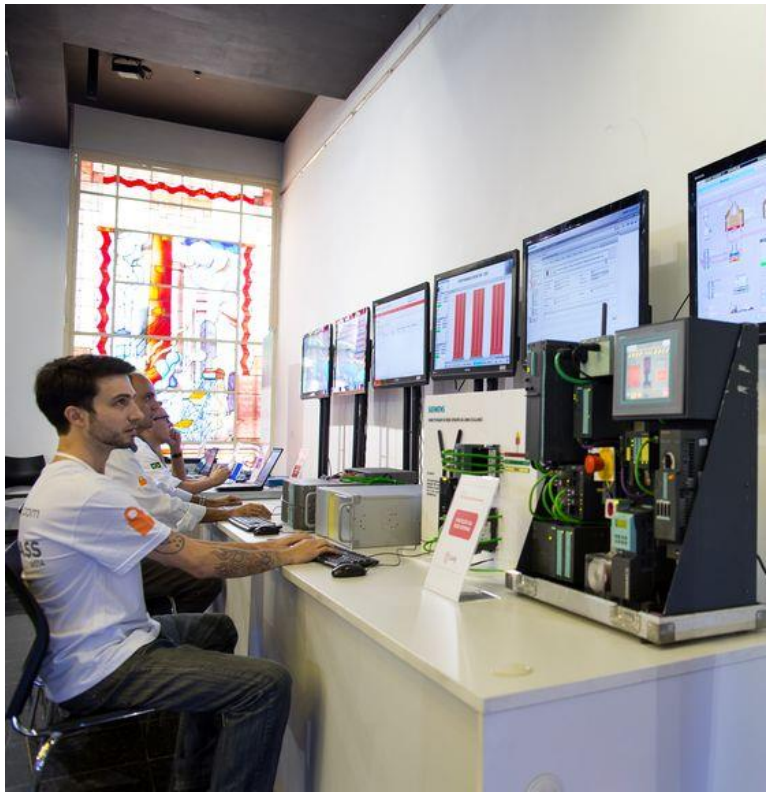
TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Principais Atividades do ICS-CERT

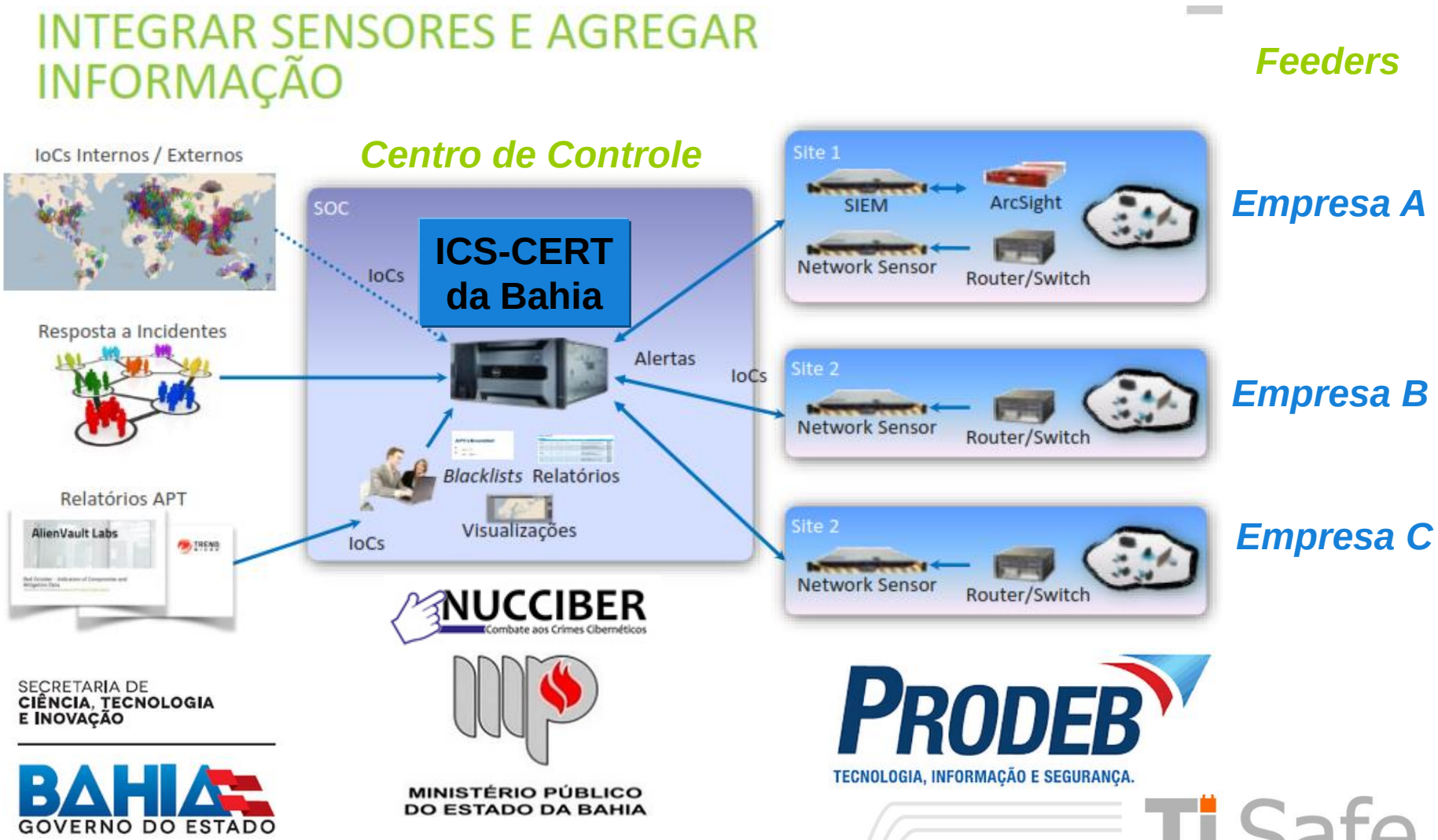
Abaixo estão os pontos prioritários do plano de ação do ICS-CERT:

- ✓**Analisar e responder sobre incidentes aos sistemas de controles industriais**
- ✓**Conduzir a análise de vulnerabilidades, malware e APTs em plantas & infraestruturas críticas**
- ✓**Prover serviços e atuação local sobre os incidentes**
- ✓**Coordenar a responsabilidade de mitigação dos riscos**
- ✓**Coordenar o compartilhamento do conhecimento referente à vulnerabilidades e incidentes reportados entre as entidades do grupo**
- ✓**Realizar trabalhos colaborativos com outros ICS-CERT no mundo**
- ✓**Promover treinamento e conscientização para os integrantes do ICS-CERT e a comunidade industrial baiana.**



TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Arquitetura de funcionamento do ICS-CERT BA



www.tisafe.com

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

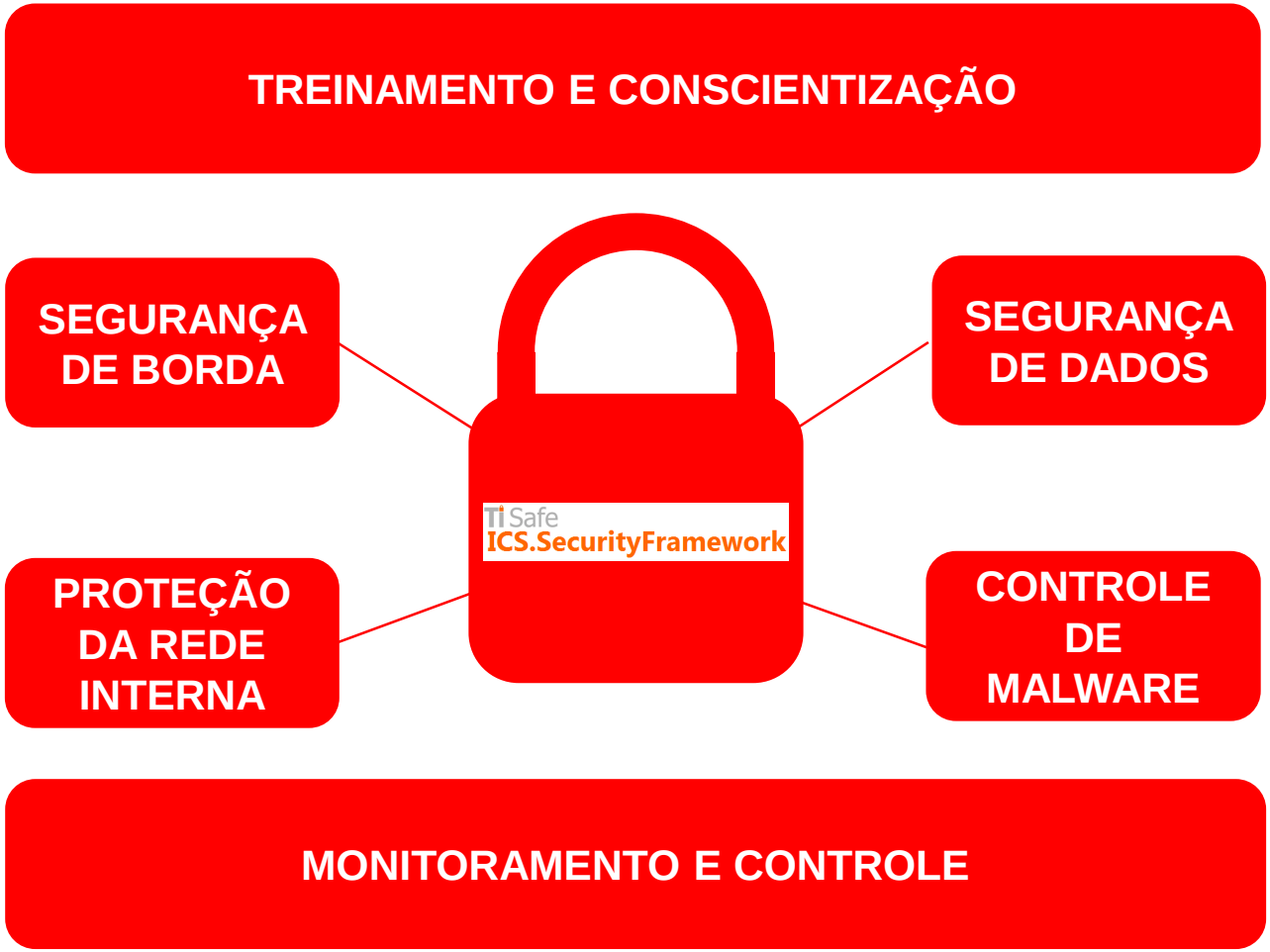
O Que é o ICS.SecurityFramework ?

É a metodologia que propõe organizar, executar e operar a segurança da informação em sistemas industriais e infraestruturas críticas:

- Implementa as boas práticas descritas no CSMS (Cyber Security Management System) da norma ANSI/ISA-99 e nas linhas base do guia NIST 800-82.
- Acelera o processo de conformidade da segurança cibernética.
- Atende às necessidades de T.I. e T.A. em um framework único.
- Provê gerenciamento centralizado do monitoramento, defesa e controle de ameaças.
- Garante a atualização das bases de dados de assinaturas e vulnerabilidades para todos os componentes de segurança.
- Facilita a identificação de ameaças e isolamento de incidentes.
- Produz trilha confiável para rastreabilidade dos eventos.
- Fornece detalhados relatórios de auditoria.

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Módulos do ICS.SecurityFramework



TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Na prática

2015 JAN - MAI

www.tisafe.com

TI Safe Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2008.Todos os direitos reservados.

Identificação de incidentes

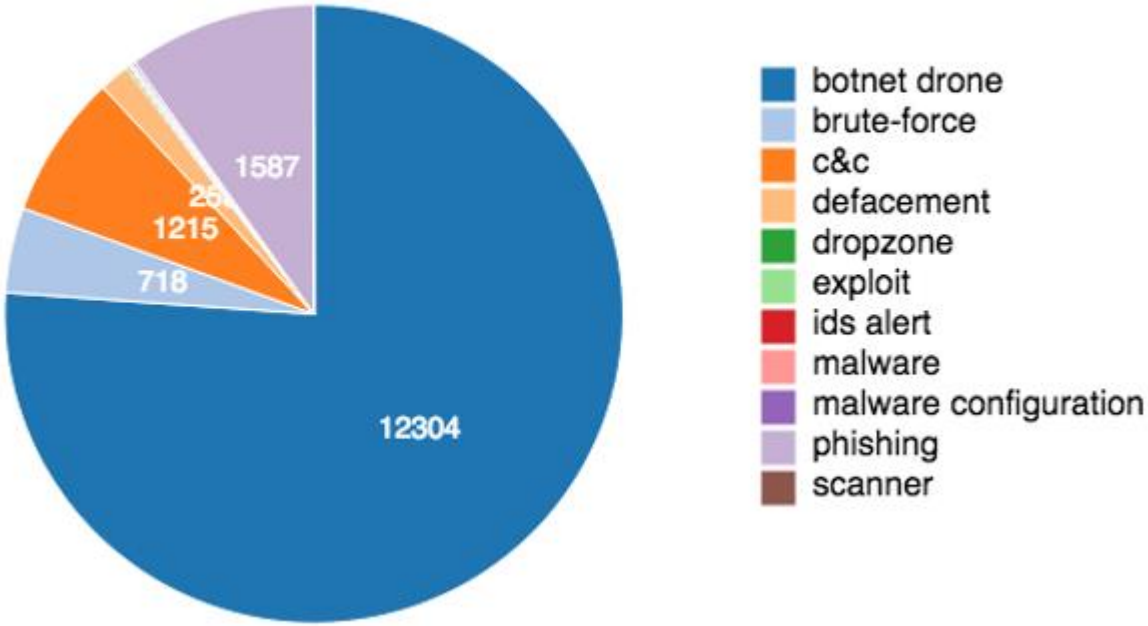
January 2015 in Brazil

280299 incident events relating to Brazil were collected and processed from ab
sources and an additional commercial sinkhole feed in January. This data does
sources that are only available to CERTs, such as the Shadowserver feeds, but rat

[redacted]

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Tipos de ataques

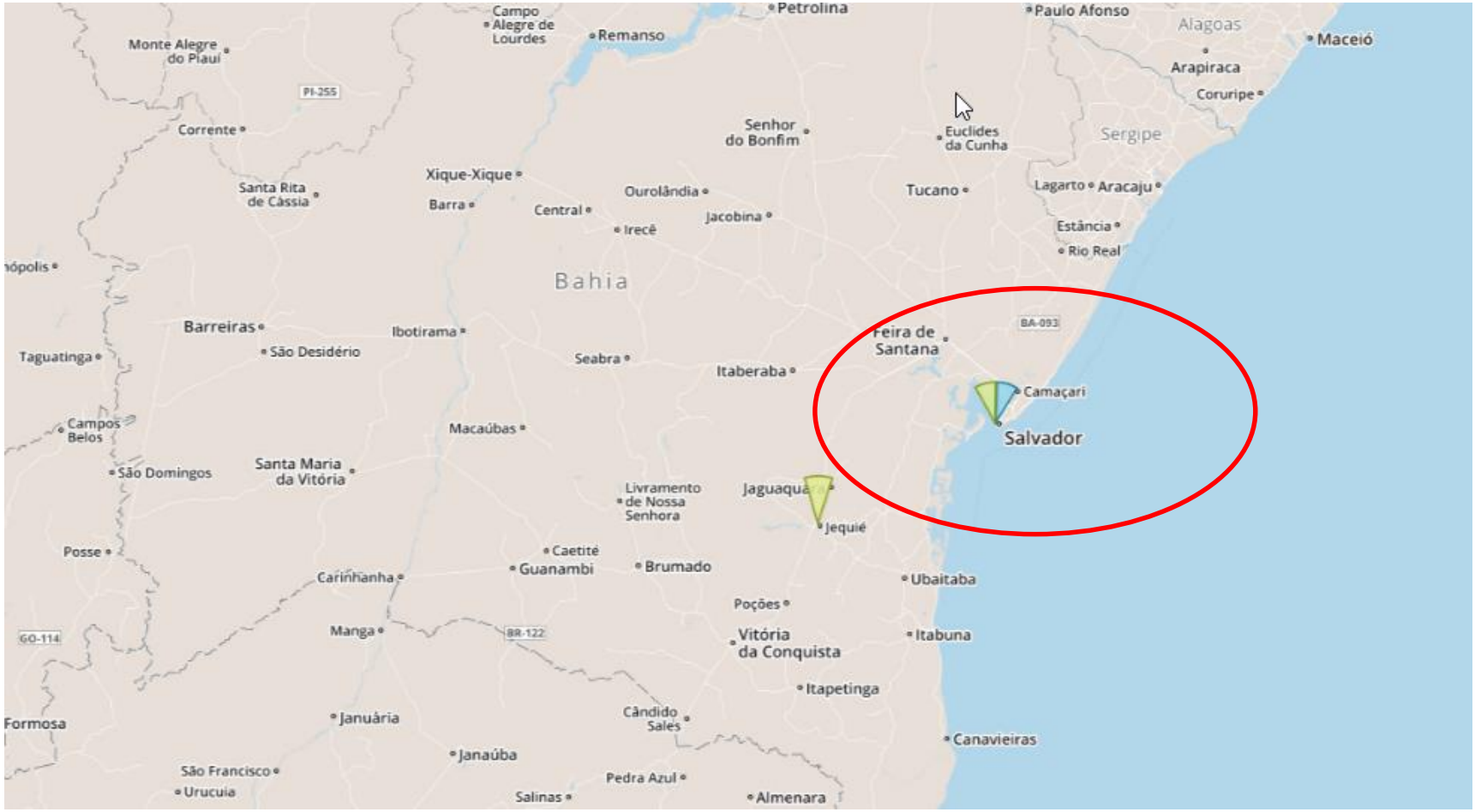


www.tisafe.com

TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Tipos de ataques por região



Região do maior Polo Petroquímico da América do Sul

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Identificação de IPs corporativos em C&C

2015-05-12 11:24:18Z	BR	200[redacted]		botnet drone	palevo	[redacted]	This host is most likely infected wi
2015-05-12 11:05:14Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-12 07:06:44Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-12 03:08:16Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 23:09:50Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 19:11:26Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 18:42:32Z	BR	177[redacted]		botnet drone	sality		This host is most likely infected wi
2015-05-11 17:39:40Z	BR	200[redacted]		botnet drone	sality		This host is most likely infected wi
2015-05-11 15:04:18Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 13:39:58Z	BR	200[redacted]		botnet drone	sality		This host is most likely infected wi
2015-05-11 11:48:17Z	BR	177[redacted]		botnet drone	sality		This host is most likely infected wi
2015-05-11 11:18:26Z	BR	200[redacted]		botnet drone	palevo		This host is most likely infected wi
2015-05-11 11:05:51Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 07:07:24Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-11 03:08:56Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 23:10:31Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 19:03:20Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 15:04:53Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 11:06:26Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 07:07:59Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-10 03:09:34Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 23:10:45Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 19:03:36Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 15:05:12Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 11:06:47Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 07:08:23Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-09 03:09:57Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-08 23:11:32Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-08 19:04:23Z	BR	200[redacted]	4	botnet drone	sality		This host is most likely infected wi
2015-05-08 17:10:14Z	BR	200[redacted]		botnet drone	sality		This host is most likely infected wi
2015-05-08 15:06:22Z	BR	177[redacted]		botnet drone	sality		This host is most likely infected wi

Indústrias invadidas por botnets C&C e que ignoravam a invasão

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Tipos de ataques por região - EUA

www.tisafe.com

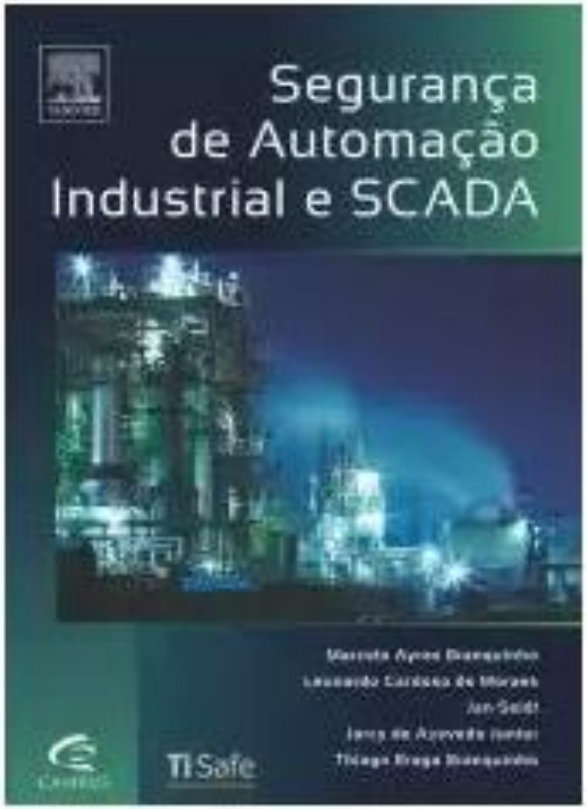
TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Hackers já causaram danos no Brasil?

- Duração: 2:22
- Este vídeo mostra reportagem do RJTV onde uma estação de tratamento de águas foi comprometida, explodiu e levou danos à sociedade.
- Discute-se que pode ter sido um ciber ataque.
- Áudio: português

Publicação do livro sobre o tema SCADA



Única publicação em língua portuguesa sobre o tema da segurança em SCADA

www.tisafe.com

TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.

Contatos

Contato

| Contato

Rio de Janeiro

Centro Empresarial Cittá America – Barra da Tijuca
Av. das Américas, 700, bloco 01, sala 331
CEP – 22640-100 – Rio de Janeiro, RJ – Brasil
Telefone: +55 (21) 2173-1159
Fax: (21) 2173-1165

São Paulo

Rua Dr. Guilherme Bannitz, nº 126 – 2º andar
Cj 21, CV 9035 – Itaim Bibi
CEP – 04532-060 – São Paulo, SP – Brasil
Telefone: +55 (11) 3040-8656
Fax: (11) 3040-8656

Salvador

Av. Tancredo Neves nº 450 – 16º andar – Edifício Suarez Trade
CEP – 41820-901 – Salvador, BA – Brasil
Telefone: +55 (71) 3340-0633
Fax: (71) 3040-0699

Na web

- Twitter: @tisafe
- Skype: ti-safe

www.tisafe.com

TI Safe
Segurança da Informação

TI Safe Segurança da Informação LTDA, 2007-2010.Todos os direitos reservados.